CLAIMS

1. Computing device with user interface comprising means for implementing a series of applications, these means including in particular a virtual machine/functioning profile execution space (100, P1, 200, P2), the device comprising a second virtual machine/functioning profile execution space (100, P1, 200, P2) differing from the first by at least its virtual machine (100, 200) or its functioning profile (P1,P2), each execution space hosting applications (110, 120, 130, 140, 220, 230), the applications of the second execution space (100, P1, 200, P2) being applications with a specifically higher level of security than the applications of the first execution space (100, P1, 200, P2) since the applications (110, 120, 130, 210, 220, 230) of the first execution space (100, P1, 200, P2) are applications which can be modified by the user, whilst the applications (110, 120, 130, 210, 220, 230) of the second execution space (100, P1, 200, P2) are applications which cannot be modified by the user, characterized in that the two execution spaces are hosted by one same physical processing means (400) which is arranged so that it cannot be separated into two parts without destroying this physical processing means (400).

2. Device as in claim 1, characterized in that the applications (110, 120, 130, 210, 220, 230) of the second execution space (100, P1, 200, P2) are applications which can be modified by a security operator belonging to the group consisting of telephony operators, banks, providers of multimedia items with selective or paying distribution, service providers operating against electronic signature via said device.

3. Device as in claim 1 or claim 2, characterized in that it forms a telephone terminal.

4. Device as in claim 3, characterized in that it forms a mobile telephony terminal.

5. Device as in any of the preceding claims, characterized in that it comprises communication means (130, 230, 300) between the two execution spaces (100, P1, 200, P2).

6. Device as in claim 5, characterized in that the communication means (130, 230, 300) between the two execution spaces are designed to authorize an application (130, 230) of one of the two execution spaces to have recourse to processing means of the second execution space (100, P1, 200, P2).

7. Device as in any of the preceding claims, characterized in that each of the two execution spaces includes at least one separate API (120, 130, 220, 230).

8. Device as in any of the preceding claims, characterized in that the communication means include an API "stub" (130, 230) whose role is to have recourse to resources of the opposite execution space (100, P1, 200, P2), these resources implementing a selection regarding access to them in relation to the caller application (110, 210).

9. Device as in any of the preceding claims, characterized in that the communication means between the two execution spaces (100, P1, 200, P2) include means implementing serialization/deserialization or marshalling/unmarshalling.

10. Device as in any of the preceding claims, characterized in that one of the two execution spaces (100, P1, 200, P2) includes a profile of STIP type.

11. Device as in any of the preceding claims, characterized in that one of the two execution spaces (100, P1, 200, P2) includes a MIDP profile.

12. Device as in any of the preceding claims, characterized in that the profiles (P1,P2) of each of the two execution spaces (100, P1, 200, P2) are respectively a STIP profile and a profile forming part of the group consisting of STIP, MIDP, OSGI and ".net" profiles.

13. Method for implementing applications within a computing device with user interface, the method having recourse to means for implementing a series of applications, these means particularly including a virtual machine /functioning profile execution space (100, P1, 200, P2), and a second virtual machine/functioning profile execution space (100, P1, 200, P2) differing from the first by at least its virtual machine (100, 200) or its functioning profile (P1,P2), each execution space (100, P1, 200, P2) hosting applications, the applications of the second execution space (100, P1, 200, P2) being applications with a specifically higher level of security than the applications of the first execution space (100, P1, 200, P2) since the applications (110, 120, 130, 210, 220, 230) of the first execution space (100, P1, 200, P2) are applications which can be modified by the user, whilst the applications (110, 120, 130, 210, 220, 230) of the second execution space (100, P1, 200, P2) are applications which cannot be modified by the user, characterized in that the two execution spaces are hosted by one same physical processing

means (400) which is arranged so that it cannot be separated into two parts without destroying this physical processing means (400).